AIRLOCK®
SECURE ACCESS HUB

FACTSHEET

Erkennung von Bots mit Machine Learning

Airlock Anomaly Shield

www.airlock.com

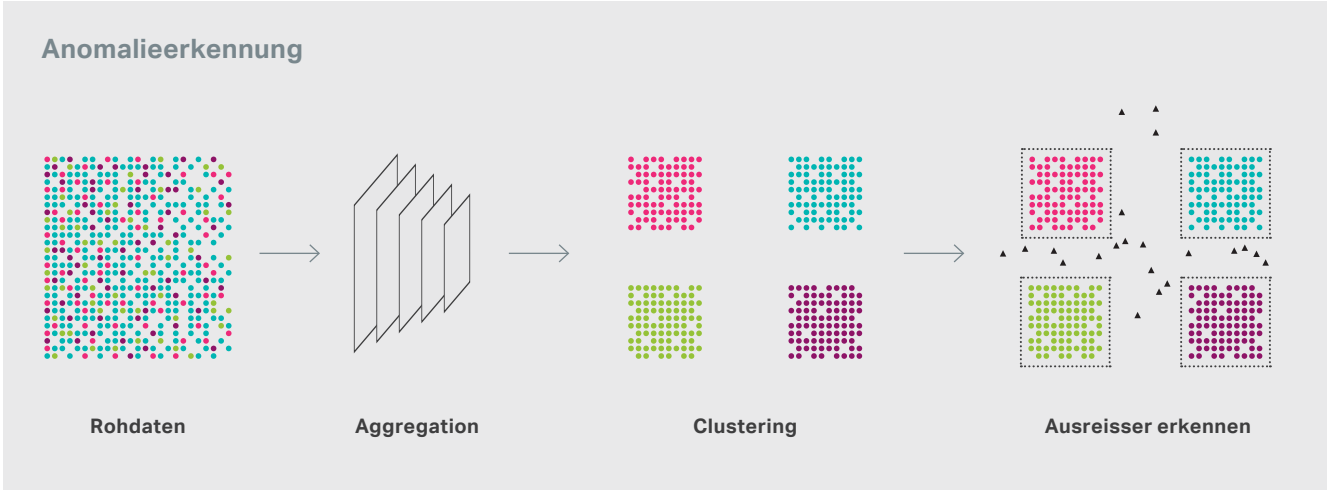
Beim «Forechecking» wird der sportliche Gegner schon gestört, bevor er überhaupt einen Angriff starten kann. Airlock Anomaly Shield erkennt unerwünschte Bots und automatisierte Attacken aufgrund ihres Verhaltens und erstickt unerwünschte Aktionen im Keim. Die verhaltensbasierte Anomalieerkennung ergänzt den klassischen, regelbasierten Schutz von Webanwendungen und APIs.

Anomalieerkennung und Bot-Management

Web Application Firewalls und API Gateways inspizieren jeden einzelnen Request und entscheiden meist sofort, ob es sich um einen Angriff handelt oder ob der Request weitergeleitet wird. Diese regelbasierten Schutzsysteme schützen insbesondere vor bekannten Angriffsarten sehr zuverlässig. Bösartige Bots und automatisierte Angriffe geben sich allerdings nicht so einfach zu erkennen. Deshalb ist hier ein anderer Ansatz erforderlich. Die Aktionen eines Bots lassen sich erst von einem richtigen Benutzer unterscheiden, wenn man das Verhalten über mehrere Requests hinweg analysiert. Die Anomalieerkennung zielt darauf ab, die Merkmale von legitimem Datenverkehr als Referenz zu modellieren. Wenn man die automatisierten Bot-Anfragen mit dem Referenzmodell vergleicht, kann man die Bots als Ausreisser erkennen und bekämpfen. Airlock Anomaly Shield erkennt bösartige Bots, automatisierte Attacken oder Schwachstellen-Scans zuverlässig innerhalb weniger Requests.

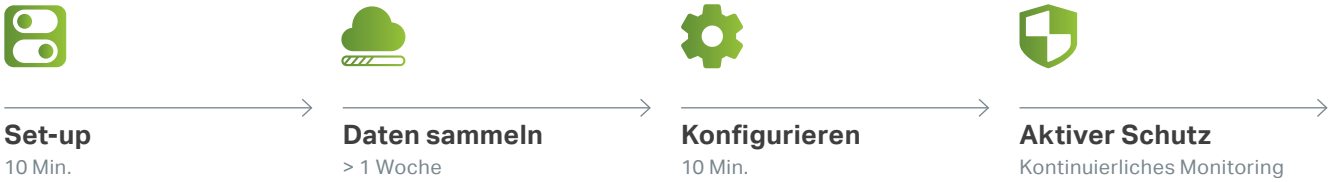
Einsatzgebiet

- Bekämpfung automatisierter Angriffe
- Erkennung und Abwehr von unerwünschten Bots wie Content Scraping, Denial of Service, Credential Stuffing usw.
- Forechecking: Abschreckung von Hackern in der Aufklärungsphase, z.B. durch das Verhindern von Vulnerability Scans.



So funktioniert Airlock Anomaly Shield

Airlock Anomaly Shield lernt während der Inbetriebnahme, wie sich die echten Benutzer einer Anwendung verhalten. Für das Unsupervised Learning werden die Rohdaten platzsparend aufbereitet und aggregiert, um die Präzision und Trefferquote zu optimieren. Die in der Trainingsphase gelernten Machine Learning Modelle bilden passgenau die Charakteristika der Businessanwendung ab. Im Betrieb werden alle aktiven Sitzungen permanent mit dem gelernten Verhalten verglichen. Wenn die Abweichung zu gross ist, wird die Sitzung als Ausreisser gekennzeichnet. Ob eine Anomalie nur protokolliert wird, oder ob die Sitzung terminiert und die IP-Adresse blockiert wird, lässt sich für jede Anwendung getrennt steuern.



Bösartige Bots: Eigenschaften und Beispiele

Bots agieren häufig sehr nahe am menschlichen Benutzerverhalten. Trotzdem lassen sie sich an ihrem Verhalten erkennen. Die folgenden Anomalien treten bei der Analyse von Bot-Traffic sehr häufig auf:

- **Ungewöhnlich viele Seitenaufrufe** innert kurzer Zeit
- **Unerwartet hohe Fehlerquote** oder Absprungrate
- **Ungewöhnliche Abfolge der Seitenaufrufe**
- **Auffällige Absenderadressen** oder TLS-Sessions

Schwachstellenscanner

Hacker verwenden automatisierte Werkzeuge, um verwundbare Systeme zu finden. Mithilfe von Bots untersuchen sie damit oft viele Systeme gleichzeitig auf mögliche Sicherheitslücken. Die einzelnen Schritte eines Scans sind oft nicht eindeutig als Angriff zu erkennen – schliesslich will der Angreifer will ja möglichst lange unter dem Radar bleiben.

Web und API Scraping

Beim Content Scraping lädt ein Bot alle Inhalte einer Website häufig mit dem Ziel herunter, die gewonnenen Daten zu missbrauchen. Auch hier bemüht sich der Angreifer, so zu tun als wäre er ein normaler Benutzer. Um die grosse Datenmenge zu bewältigen, sind allerdings viel mehr Seitenaufrufe notwendig. Airlock Anomaly Shield wurde entwickelt, um solche Scraping-Angriffe und andere Arten von böswilligem Traffic zu bekämpfen.

Credential Stuffing

Beim Credential Stuffing wird ausgenutzt, dass das gleiche Passwort aus Bequemlichkeit oft für mehrere Dienste verwendet wird. Angreifer können so versuchen, Benutzerkonten zu kompromittieren, indem sie gestohlene Anmeldeinformationen auf anderen Systemen ausprobieren. Der stärkste Schutz gegen Credential Stuffing ist die Abwehr von Bots. Als Gegenmassnahme kommen auch Zwei-Faktor-Authentifizierung oder CAPTCHAs infrage. Diese werden aber von den Endbenutzern oft als lästig empfunden.

Denial-of-Service Angriffe

Bei einem Denial-of-Service-Angriff (DoS) versucht ein böswilliger Akteur, einen Dienst für seine vorgesehenen Benutzer unzugänglich zu machen. Das System wird mit Anfragen überflutet, bis der normale Datenverkehr nicht mehr verarbeitet werden kann. Durch Verhaltensanalyse können DoS-Angriffe erkannt und aufgehalten werden, bevor sie Schaden einrichten.

Vorteile

- **Schnelle Inbetriebnahme ohne Data Science Know-how:** Wartung und Einrichtung sind innerhalb von Minuten möglich, auch ohne Kenntnisse in Machine Learning.
- **Abwehr unbekannter Angriffsarten:** Das anwendungsspezifische Training resultiert in einem positiven Sicherheitsmodell. Damit können auch unbekannte Bots oder Zero-Day-Attacken erkannt werden, weil der Schutz nicht auf Signaturen basiert.
- **100 % Datenschutz und Kontrolle:** Das gelernte Verhalten sowie die Anomalie-Entscheidungen verlassen den Airlock Gateway Cluster nicht.
- **Einstellbare Empfindlichkeit:** Bei einer Häufung von False Positives/Negatives kann die Sensitivität für jeden Sensor angepasst werden.
- **Hoher Datendurchsatz:** Die Analyse erfolgt im Hintergrund und entkoppelt vom normalen Datenfluss. Eine Verzögerung des Datenverkehrs ist durch die asynchrone Beurteilung ausgeschlossen.

Umfassender Bot-Schutz

Für den optimalen Anwendungsschutz empfiehlt sich die Kombination verschiedener Bot Management Funktionen im Airlock Secure Access Hub®:

- **Threat Intelligence:** Der BrightCloud Threat Intelligence Service von Webroot verwendet Echtzeit-Reputationsdaten, um unerwünschte IP-Adressen zu blockieren.
- **DoS-Schutz mit Rate Limiting:** Sind die Anzahl Requests oder Sessions pro IP besonders hoch, verhindert der DoS-Schutz, dass Anwendungen überlastet werden. Insbesondere bei APIs wird der Datendurchsatz auch abhängig von der Benutzeridentität begrenzt.
- **Vorgelagerte Authentifizierung:** Damit nur berechtigte Benutzer auf die Anwendung zugreifen können, werden nicht identifizierte Besucher z. B. auf die Anmeldeseite von Airlock IAM umgeleitet.
- **Bot Management:** Erkennt Bots und kann verlangen, dass alle Aufrufer Cookies retournieren. Viele automatisierte Bots können diese Hürde nicht nehmen, da sie keinen Cookie Store haben. Search Engine Bots müssen zudem aus dem IP Range der jeweiligen Search Engine zugreifen. Bei wiederholten Verstössen gegen die Sicherheitsregeln innerhalb kurzer Zeit wird eine IP in Quarantäne gestellt. Während der Quarantäne werden keine Requests von diesen IPs mehr entgegengenommen.

Ergänzung mit zusätzlichen Bot-Schutzmassnahmen

Möchten Sie Airlock Anomaly Shield ausprobieren?

Wenn Sie Interesse an Airlock Anomaly Shield haben, kontaktieren Sie uns via E-Mail an **order@airlock.com**.
Wir stellen Ihnen gerne eine Testlizenz aus, um die Bot-Erkennung im Log-only-Modus zu testen.

Copyright © 2022 Ergon Informatik AG. All Rights Reserved. All technical documentation that is made available by Ergon Informatik AG is the copyrighted work of Ergon Informatik AG and is owned by Ergon Informatik AG. Ergon, the Ergon logo, «smart people – smart software» and Airlock are registered trademarks of Ergon Informatik AG. Microsoft and ActiveDirectory are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other products or trademarks mentioned are the property of their respective owners.